(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2000137681 A

(43) Date of publication of application: 16 . 05 . 00

(51) Int. Cl G06F 15/00
G06F 19/00
G09C 1/00
H04L 9/32

(21) Application number: 10310686

(22) Date of filing: 30 . 10 . 98

(71) Applicant: TOSHIBA CORP

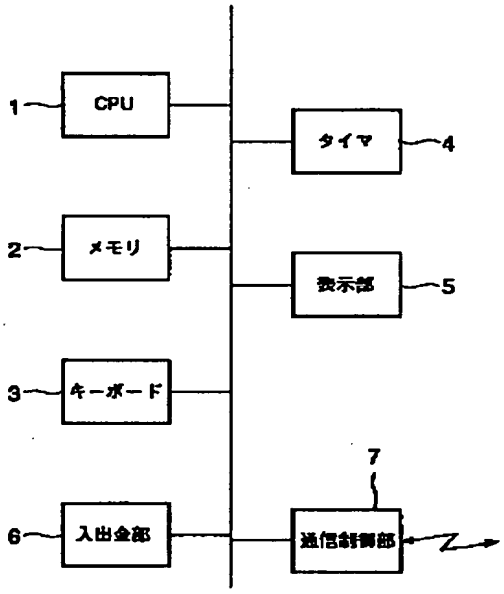
(72) Inventor: SHIMIZU MAKOTO

(54) INDIVIDUAL AUTHENTICATION METHOD AND DEVICE

(57) Abstract:

PROBLEM TO BE SOLVED: To provide an individual authentication method and device capable of preventing illegal use due to impersonation into the person himself, and improving the precision of individual authentication.

SOLUTION: A character input interval at the time of the password data input of a person to be authenticated is preliminarily registered. When the person to be authenticated inputs the password data, the character input interval is measured, and collated with the preliminarily registered character input terminal, and when the inputted password data is coincident with the registered password data, and the measured character input interval is coincident with the registered character input interval within the range of a preliminarily set allowable error value, it is authenticated that the person to be authenticated is the person himself.



(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開２０００－１３７６８１
(Ｐ２０００－１３７６８１Ａ)
(43)公開日　平成12年5月16日(2000.5.16)

(51)Int.Cl.⁷		識別記号	FI			テーマコード(参考)
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｂ	5B055
	19/00		Ｇ０９Ｃ	1/00	６４０Ａ	5B085
Ｇ０９Ｃ	1/00	６４０	Ｇ０６Ｆ	15/30	３４０	5J104
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７３Ａ	9A001
					６７５Ａ	

審査請求　未請求　請求項の数１６　ＯＬ　(全１５頁)

(21)出願番号　特願平10-310686

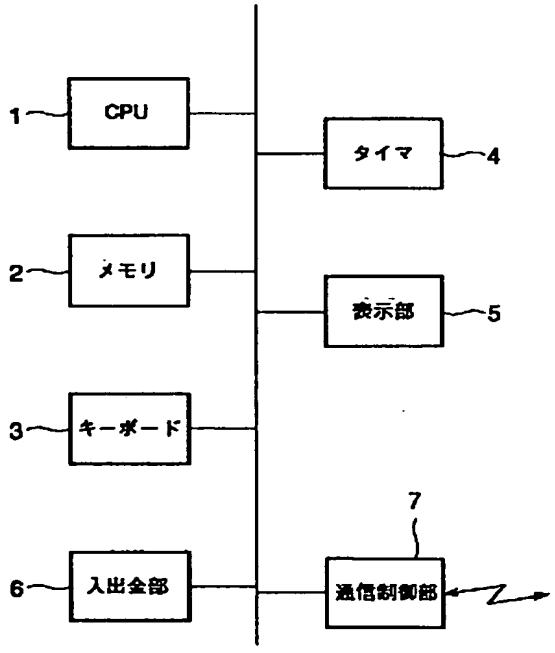
(22)出願日　平成10年10月30日(1998.10.30)

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　清水　眞
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内
(74)代理人　100058479
弁理士　鈴江　武彦　(外6名)

Ｆターム(参考)　5B055 BB10 HA04 HA17 HB01
5B085 AE03 AE15 AE23 AE29
5J104 AA07 KA01 KA04 KA14 NA05
9A001 JJ58 JJ65 LL03

(54)【発明の名称】個人認証方法および個人認証装置

(57)【要約】
【課題】本人へのなりすましによる不正使用を防止でき、個人認証の精度が著しく向上する個人認証方法および個人認証装置を提供する。
【解決手段】被認証者のパスワードデータ入力時における文字入力間隔をあらかじめ登録しておき、被認証者が行なうパスワードデータ入力の際にその文字入力間隔をそれぞれ計測して、あらかじめ登録された文字入力間隔と照合することにより、入力されたパスワードデータと登録されたパスワードデータとが一致し、かつ、計測された文字入力間隔と登録された文字入力間隔とがあらかじめ設定される許容誤差値の範囲内で一致した場合に被認証者が本人であると認証する。



1

【特許請求の範囲】

【請求項１】　被認証者の複数の文字からなるパスワードデータを１文字ずつ入力し、

このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測し、

この入力されたパスワードデータおよび計測された文字入力間隔をあらかじめ登録されているパスワードデータおよび文字入力間隔とそれぞれ照合し、

この照合において、前記入力されたパスワードデータおよび計測された文字入力間隔と前記登録されているパスワードデータおよび文字入力間隔との間に所定の関係が成立するか否かにより、前記被認証者が本人であるか否かの認証を行なうことを特徴とする個人認証方法。

【請求項２】　被認証者の複数の文字からなるパスワードデータを１文字ずつ入力し、

このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測し、

この入力されたパスワードデータおよび計測された文字入力間隔をあらかじめ登録されているパスワードデータおよび文字入力間隔とそれぞれ照合し、

この照合において、前記入力されたパスワードデータと前記登録されているパスワードデータとの間に所定の関係が成立し、かつ、前記計測された文字入力間隔と前記登録されている文字入力間隔とがあらかじめ設定される許容誤差値の範囲内で一致した場合に前記被認証者が本人であると認証することを特徴とする個人認証方法。

【請求項３】　前記パスワードデータの入力時、計時手段により１文字ごとの入力時刻を得て、これら得た入力時刻の間で演算を行なうことにより各文字の入力間隔を算出することを特徴とする請求項１または２記載の個人認証方法。

【請求項４】　登録時、登録用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力するステップと、

このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、

前記入力されたパスワードデータおよび計測された文字入力間隔を登録データとして記憶手段に登録記憶するステップと、

照合時、照合用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力するステップと、

このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、

前記入力された照合用のパスワードデータおよび計測された文字入力間隔を前記記憶手段に登録されたパスワードデータおよび文字入力間隔とそれぞれ照合するステップと、

この照合において、前記入力された照合用のパスワードデータおよび計測された文字入力間隔と前記記憶手段に登録されたパスワードデータおよび文字入力間隔との間

2

に所定の関係が成立するか否かにより、前記被認証者が本人であるか否かの認証を行なうステップと、

からなることを特徴とする個人認証方法。

【請求項５】　登録時、登録用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力するステップと、

このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、

文字入力間隔の許容誤差値を入力するステップと、

前記入力されたパスワードデータおよび計測された文字入力間隔および入力された許容誤差値を登録データとして記憶手段に登録記憶するステップと、

照合時、照合用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力するステップと、

このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、

前記入力された照合用のパスワードデータおよび計測された文字入力間隔を前記記憶手段に登録されたパスワードデータおよび文字入力間隔とそれぞれ照合するステップと、

この照合において、前記入力されたパスワードデータと前記記憶手段に登録されたパスワードデータとの間に所定の関係が成立し、かつ、前記計測された文字入力間隔と前記記憶手段に登録された文字入力間隔とが前記記憶手段に登録された許容誤差値の範囲内で一致した場合に前記被認証者が本人であると認証するステップと、

からなることを特徴とする個人認証方法。

【請求項６】　前記パスワードデータの入力時、計時手段により１文字ごとの入力時刻を得て、これら得た入力時刻の間で演算を行なうことにより各文字の入力間隔を算出することを特徴とする請求項４または５記載の個人認証方法。

【請求項７】　前記許容誤差値の入力において、許容誤差値の上限値および下限値のうち少なくともいずれか一方を設けることにより、これを超える値の指定を禁止するようにしたことを特徴とする請求項５記載の個人認証方法。

【請求項８】　登録時、被認証者を特定するための識別情報を入力するステップと、

登録用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力するステップと、

このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、

前記入力された識別情報およびパスワードデータおよび計測された文字入力間隔を登録データとして記憶手段に登録記憶するステップと、

照合時、被認証者を特定するための識別情報を入力するステップと、

照合用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力するステップと、

このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、
前記入力された照合用の識別情報およびパスワードデータおよび計測された文字入力間隔を前記記憶手段に登録された識別情報およびパスワードデータおよび文字入力間隔とそれぞれ照合するステップと、
この照合において、前記入力された照合用の識別情報およびパスワードデータおよび計測された文字入力間隔と前記記憶手段に登録された識別情報およびパスワードデータおよび文字入力間隔との間に所定の関係が成立するか否かにより、前記被認証者が本人であるか否かの認証を行なうステップと、
からなることを特徴とする個人認証方法。

【請求項９】　登録時、被認証者を特定するための識別情報を入力するステップと、
登録用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力するステップと、
このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、
文字入力間隔の許容誤差値を入力するステップと、
前記入力された識別情報およびパスワードデータおよび計測された文字入力間隔および入力された許容誤差値を登録データとして記憶手段に登録記憶するステップと、
照合時、被認証者を特定するための識別情報を入力するステップと、
照合用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力するステップと、
このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、
前記入力された照合用の識別情報およびパスワードデータおよび計測された文字入力間隔を前記記憶手段に登録された識別情報およびパスワードデータおよび文字入力間隔とそれぞれ照合するステップと、
この照合において、前記入力された識別情報およびパスワードデータと前記記憶手段に登録された識別情報およびパスワードデータとの間に所定の関係が成立し、かつ、前記計測された文字入力間隔と前記記憶手段に登録された文字入力間隔とが前記記憶手段に登録された許容誤差値の範囲内で一致した場合に前記被認証者が本人であると認証するステップと、
からなることを特徴とする個人認証方法。

【請求項１０】　あらかじめ定められた特定の識別情報が入力された場合に前記文字入力間隔の計測および照合を行なわないようにしたことを特徴とする請求項８または９記載の個人認証方法。

【請求項１１】　被認証者の複数の文字からなるパスワードデータを１文字ずつ入力するパスワード入力手段と、
このパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する入力間隔計測手段と、
前記パスワード入力手段により入力されたパスワードデータおよび前記入力間隔計測手段により計測された文字入力間隔をあらかじめ登録されているパスワードデータおよび文字入力間隔とそれぞれ照合する照合手段と、
この照合手段の照合において、前記パスワード入力手段により入力されたパスワードデータおよび前記入力間隔計測手段により計測された文字入力間隔と前記登録されているパスワードデータおよび文字入力間隔との間に所定の関係が成立するか否かにより、前記被認証者が本人であるか否かの認証を行なう認証手段と、
を具備したことを特徴とする個人認証装置。

【請求項１２】　被認証者の複数の文字からなるパスワードデータを１文字ずつ入力するパスワード入力手段と、
このパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する入力間隔計測手段と、
前記パスワード入力手段により入力されたパスワードデータおよび前記入力間隔計測手段により計測された文字入力間隔をあらかじめ登録されているパスワードデータおよび文字入力間隔とそれぞれ照合する照合手段と、
この照合手段の照合において、前記パスワード入力手段により入力されたパスワードデータと前記登録されているパスワードデータとの間に所定の関係が成立し、かつ、前記入力間隔計測手段により計測された文字入力間隔と前記登録されている文字入力間隔とがあらかじめ設定される許容誤差値の範囲内で一致した場合に前記被認証者が本人であると認証する認証手段と、
を具備したことを特徴とする個人認証装置。

【請求項１３】　登録時、登録用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力する第１のパスワード入力手段と、
この第１のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第１の入力間隔計測手段と、
前記第１のパスワード入力手段により入力されたパスワードデータおよび前記第１の入力間隔計測手段により計測された文字入力間隔を登録データとして登録記憶する記憶手段と、
照合時、照合用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力する第２のパスワード入力手段と、
この第２のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第２の入力間隔計測手段と、
前記第２のパスワード入力手段により入力された照合用のパスワードデータおよび前記第２の入力間隔計測手段により計測された文字入力間隔を前記記憶手段に登録されたパスワードデータおよび文字入力間隔とそれぞれ照

合する照合手段と、
この照合手段の照合において、前記第２のパスワード入力手段により入力された照合用のパスワードデータおよび前記第２の入力間隔計測手段により計測された文字入力間隔と前記記憶手段に登録されたパスワードデータおよび文字入力間隔との間に所定の関係が成立するか否かにより、前記被認証者が本人であるか否かの認証を行なう認証手段と、
を具備したことを特徴とする個人認証装置。
【請求項１４】　登録時、登録用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力する第１のパスワード入力手段と、
この第１のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第１の入力間隔計測手段と、
文字入力間隔の許容誤差値を入力する許容誤差値入力手段と、
前記第１のパスワード入力手段により入力されたパスワードデータおよび前記第１の入力間隔計測手段により計測された文字入力間隔および前記入力間隔計測手段により入力された許容誤差値を登録データとして登録記憶する記憶手段と、
照合時、照合用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力する第２のパスワード入力手段と、
この第２のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第２の入力間隔計測手段と、
前記第２のパスワード入力手段により入力された照合用のパスワードデータおよび前記第２の入力間隔計測手段により計測された文字入力間隔を前記記憶手段に登録されたパスワードデータおよび文字入力間隔とそれぞれ照合する照合手段と、
この照合手段の照合において、前記第２のパスワード入力手段により入力されたパスワードデータと前記記憶手段に登録されたパスワードデータとの間に所定の関係が成立し、かつ、前記第２の入力間隔計測手段により計測された文字入力間隔と前記記憶手段に登録された文字入力間隔とが前記記憶手段に登録された許容誤差値の範囲内で一致した場合に前記被認証者が本人であると認証する認証手段と、
を具備したことを特徴とする個人認証装置。
【請求項１５】　登録時、被認証者を特定するための識別情報を入力する第１の識別情報入力手段と、
登録用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力する第１のパスワード入力手段と、
この第１のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第１の入力間隔計測手段と、
前記第１の識別情報入力手段により入力された識別情報および前記第１のパスワード入力手段により入力されたパスワードデータおよび前記第１の入力間隔計測手段により計測された文字入力間隔を登録データとして登録記憶する記憶手段と、
照合時、被認証者を特定するための識別情報を入力する第２の識別情報入力手段と、
照合用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力する第２のパスワード入力手段と、
この第２のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第２の入力間隔計測手段と、
前記第２の識別情報入力手段により入力された照合用の識別情報および前記第２のパスワード入力手段により入力されたパスワードデータおよび前記第２の入力間隔計測手段により計測された文字入力間隔を前記記憶手段に登録された識別情報およびパスワードデータおよび文字入力間隔とそれぞれ照合する照合手段と、
この照合手段の照合において、前記第２の識別情報入力手段により入力された照合用の識別情報および前記第２のパスワード入力手段により入力されたパスワードデータおよび前記第２の入力間隔計測手段により計測された文字入力間隔と前記記憶手段に登録された識別情報およびパスワードデータおよび文字入力間隔との間に所定の関係が成立するか否かにより、前記被認証者が本人であるか否かの認証を行なう認証手段と、
を具備したことを特徴とする個人認証装置。
【請求項１６】　登録時、被認証者を特定するための識別情報を入力する第１の識別情報入力手段と、
登録用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力する第１のパスワード入力手段と、
この第１のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第１の入力間隔計測手段と、
文字入力間隔の許容誤差値を入力する許容誤差値入力手段と、
前記第１の識別情報入力手段により入力された識別情報および前記第１のパスワード入力手段により入力されたパスワードデータおよび前記第１の入力間隔計測手段により計測された文字入力間隔および前記許容誤差値入力手段により入力された許容誤差値を登録データとして登録記憶する記憶手段と、
照合時、被認証者を特定するための識別情報を入力する第２の識別情報入力手段と、
照合用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力する第２のパスワード入力手段と、
この第２のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第２の入力間隔計測手段と、
前記第２の識別情報入力手段により入力された照合用の識別情報および前記第２のパスワード入力手段により入

力されたパスワードデータおよび前記第２の入力間隔計測手段により計測された文字入力間隔を前記記憶手段に登録された識別情報およびパスワードデータおよび文字入力間隔とそれぞれ照合する照合手段と、
この照合手段の照合において、前記第２の識別情報入力手段により入力された識別情報および前記第２のパスワード入力手段により入力されたパスワードデータと前記記憶手段に登録された識別情報およびパスワードデータとの間に所定の関係が成立し、かつ、前記第２の入力間隔計測手段により計測された文字入力間隔と前記記憶手段に登録された文字入力間隔とが前記記憶手段に登録された許容誤差値の範囲内で一致した場合に前記被認証者が本人であると認証する認証手段と、
を具備したことを特徴とする個人認証装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、たとえば、現金処理機やキャッシュレジスタなどの現金の出入りを管理する端末装置などにおいて、オペレータが使用を許可された者であるか否かの個人認証を行なう個人認証方法および個人認証装置に関する。
【０００２】
【従来の技術】たとえば、現金の出入りを管理する現金処理機やキャッシュレジスタ、あるいは、機密情報を保管・表示・操作するパーソナルコンピュータなどの端末装置は、あらかじめ使用を許可された特定のオペレータ（以降、利用者と言うこともある）以外が不正に使用することを防止するため、使用に先立ちパスワードデータのチェックを行なうことが多い。このパスワードデータは、オペレータごとに定められていて、通常は数字や文字もしくはその両者の組合わせからなる。なお、以降、数字と文字を総称して文字と記す。
【０００３】
【発明が解決しようとする課題】ところが、パスワードデータのチェックは、簡便な反面、パスワードデータを盗み見られてしまうと、本人へのなりすましによる不正使用が可能になり、個人認証の精度が著しく低下するという大きな問題がある。
【０００４】そこで、本発明は、本人へのなりすましによる不正使用を防止でき、個人認証の精度が著しく向上する個人認証方法および個人認証装置を提供することを目的とする。
【０００５】
【課題を解決するための手段】本発明の個人認証方法は、被認証者の複数の文字からなるパスワードデータを１文字ずつ入力し、このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測し、この入力されたパスワードデータおよび計測された文字入力間隔をあらかじめ登録されているパスワードデータおよび文字入力間隔とそれぞれ照合し、この照合において、前記入力されたパスワードデータおよび計測された文字入力間隔と前記登録されているパスワードデータおよび文字入力間隔との間に所定の関係が成立するか否かにより、前記被認証者が本人であるか否かの認証を行なうことを特徴とする。
【０００６】また、本発明の個人認証方法は、被認証者の複数の文字からなるパスワードデータを１文字ずつ入力し、このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測し、この入力されたパスワードデータおよび計測された文字入力間隔をあらかじめ登録されているパスワードデータおよび文字入力間隔とそれぞれ照合し、この照合において、前記入力されたパスワードデータと前記登録されているパスワードデータとの間に所定の関係が成立し、かつ、前記計測された文字入力間隔と前記登録されている文字入力間隔とがあらかじめ設定される許容誤差値の範囲内で一致した場合に前記被認証者が本人であると認証することを特徴とする。
【０００７】また、本発明の個人認証方法は、登録時、登録用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力するステップと、このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、前記入力されたパスワードデータおよび計測された文字入力間隔を登録データとして記憶手段に登録記憶するステップと、照合時、照合用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力するステップと、このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、前記入力された照合用のパスワードデータおよび計測された文字入力間隔を前記記憶手段に登録されたパスワードデータおよび文字入力間隔とそれぞれ照合するステップと、この照合において、前記入力された照合用のパスワードデータおよび計測された文字入力間隔と前記記憶手段に登録されたパスワードデータおよび文字入力間隔との間に所定の関係が成立するか否かにより、前記被認証者が本人であるか否かの認証を行なうステップとからなる。
【０００８】また、本発明の個人認証方法は、登録時、登録用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力するステップと、このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、文字入力間隔の許容誤差値を入力するステップと、前記入力されたパスワードデータおよび計測された文字入力間隔および入力された許容誤差値を登録データとして記憶手段に登録記憶するステップと、照合時、照合用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力するステップと、このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、前記入力された照合用のパスワードデータおよび計測された文字入力間隔を前記記憶手段に登録されたパスワードデータおよび文字入力間隔とそれぞれ照合するステップと、この照合において、前記入力されたパ

スワードデータと前記記憶手段に登録されたパスワードデータとの間に所定の関係が成立し、かつ、前記計測された文字入力間隔と前記記憶手段に登録された文字入力間隔とが前記記憶手段に登録された許容誤差値の範囲内で一致した場合に前記被認証者が本人であると認証するステップとからなる。

【０００９】また、本発明の個人認証方法は、登録時、被認証者を特定するための識別情報を入力するステップと、登録用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力するステップと、このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、前記入力された識別情報およびパスワードデータおよび計測された文字入力間隔を登録データとして記憶手段に登録記憶するステップと、照合時、被認証者を特定するための識別情報を入力するステップと、照合用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力するステップと、このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、前記入力された照合用の識別情報およびパスワードデータおよび計測された文字入力間隔を前記記憶手段に登録された識別情報およびパスワードデータおよび文字入力間隔とそれぞれ照合するステップと、この照合において、前記入力された照合用の識別情報およびパスワードデータおよび計測された文字入力間隔と前記記憶手段に登録された識別情報およびパスワードデータおよび文字入力間隔との間に所定の関係が成立するか否かにより、前記被認証者が本人であるか否かの認証を行なうステップとからなる。

【００１０】また、本発明の個人認証方法は、登録時、被認証者を特定するための識別情報を入力するステップと、登録用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力するステップと、このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、文字入力間隔の許容誤差値を入力するステップと、前記入力された識別情報およびパスワードデータおよび計測された文字入力間隔および入力された許容誤差値を登録データとして記憶手段に登録記憶するステップと、照合時、被認証者を特定するための識別情報を入力するステップと、照合用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力するステップと、このパスワードデータの入力時に各文字の入力間隔をそれぞれ計測するステップと、前記入力された照合用の識別情報およびパスワードデータおよび計測された文字入力間隔を前記記憶手段に登録された識別情報およびパスワードデータおよび文字入力間隔とそれぞれ照合するステップと、この照合において、前記入力された識別情報およびパスワードデータと前記記憶手段に登録された識別情報およびパスワードデータとの間に所定の関係が成立し、かつ、前記計測された文字入力間隔と前記記憶手段に登録された文字入力間隔とが前記記憶手段に登録された許容誤差値の範囲内で一致した場合に前記被認証者が本人であると認証するステップとからなる。

【００１１】また、本発明の個人認証装置は、被認証者の複数の文字からなるパスワードデータを１文字ずつ入力するパスワード入力手段と、このパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する入力間隔計測手段と、前記パスワード入力手段により入力されたパスワードデータおよび前記入力間隔計測手段により計測された文字入力間隔をあらかじめ登録されているパスワードデータおよび文字入力間隔とそれぞれ照合する照合手段と、この照合手段の照合において、前記パスワード入力手段により入力されたパスワードデータおよび前記入力間隔計測手段により計測された文字入力間隔と前記登録されているパスワードデータおよび文字入力間隔との間に所定の関係が成立するか否かにより、前記被認証者が本人であるか否かの認証を行なう認証手段とを具備している。

【００１２】また、本発明の個人認証装置は、被認証者の複数の文字からなるパスワードデータを１文字ずつ入力するパスワード入力手段と、このパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する入力間隔計測手段と、前記パスワード入力手段により入力されたパスワードデータおよび前記入力間隔計測手段により計測された文字入力間隔をあらかじめ登録されているパスワードデータおよび文字入力間隔とそれぞれ照合する照合手段と、この照合手段の照合において、前記パスワード入力手段により入力されたパスワードデータと前記登録されているパスワードデータとの間に所定の関係が成立し、かつ、前記入力間隔計測手段により計測された文字入力間隔と前記登録されている文字入力間隔とがあらかじめ設定される許容誤差値の範囲内で一致した場合に前記被認証者が本人であると認証する認証手段とを具備している。

【００１３】また、本発明の個人認証装置は、登録時、登録用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力する第１のパスワード入力手段と、この第１のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第１の入力間隔計測手段と、前記第１のパスワード入力手段により入力されたパスワードデータおよび前記第１の入力間隔計測手段により計測された文字入力間隔を登録データとして登録記憶する記憶手段と、照合時、照合用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力する第２のパスワード入力手段と、この第２のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第２の入力間隔計測手段と、前記第２のパスワード入力手段により入力された照合用のパスワードデータおよび前記第２の入力間隔計測手段により計測された文字入力間隔を前記記憶手段に登録されたパスワードデータおよび文字入力間隔と

それぞれ照合する照合手段と、この照合手段の照合において、前記第２のパスワード入力手段により入力された照合用のパスワードデータおよび前記第２の入力間隔計測手段により計測された文字入力間隔と前記記憶手段に登録されたパスワードデータおよび文字入力間隔との間に所定の関係が成立するか否かにより、前記被認証者が本人であるか否かの認証を行なう認証手段とを具備している。

【００１４】また、本発明の個人認証装置は、登録時、登録用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力する第１のパスワード入力手段と、この第１のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第１の入力間隔計測手段と、文字入力間隔の許容誤差値を入力する許容誤差値入力手段と、前記第１のパスワード入力手段により入力されたパスワードデータおよび前記第１の入力間隔計測手段により計測された文字入力間隔および前記入力間隔計測手段により入力された許容誤差値を登録データとして登録記憶する記憶手段と、照合時、照合用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力する第２のパスワード入力手段と、この第２のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第２の入力間隔計測手段と、前記第２のパスワード入力手段により入力された照合用のパスワードデータおよび前記第２の入力間隔計測手段により計測された文字入力間隔を前記記憶手段に登録されたパスワードデータおよび文字入力間隔とそれぞれ照合する照合手段と、この照合手段の照合において、前記第２のパスワード入力手段により入力されたパスワードデータと前記記憶手段に登録されたパスワードデータとの間に所定の関係が成立し、かつ、前記第２の入力間隔計測手段により計測された文字入力間隔と前記記憶手段に登録された文字入力間隔とが前記記憶手段に登録された許容誤差値の範囲内で一致した場合に前記被認証者が本人であると認証する認証手段とを具備している。

【００１５】また、本発明の個人認証装置は、登録時、被認証者を特定するための識別情報を入力する第１の識別情報入力手段と、登録用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力する第１のパスワード入力手段と、この第１のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第１の入力間隔計測手段と、前記第１の識別情報入力手段により入力された識別情報および前記第１のパスワード入力手段により入力されたパスワードデータおよび前記第１の入力間隔計測手段により計測された文字入力間隔を登録データとして登録記憶する記憶手段と、照合時、被認証者を特定するための識別情報を入力する第２の識別情報入力手段と、照合用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力する第２のパスワード入力手段と、この第２のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第２の入力間隔計測手段と、前記第２の識別情報入力手段により入力された照合用の識別情報および前記第２のパスワード入力手段により入力されたパスワードデータおよび前記第２の入力間隔計測手段により計測された文字入力間隔を前記記憶手段に登録された識別情報およびパスワードデータおよび文字入力間隔とそれぞれ照合する照合手段と、この照合手段の照合において、前記第２の識別情報入力手段により入力された照合用の識別情報および前記第２のパスワード入力手段により入力されたパスワードデータおよび前記第２の入力間隔計測手段により計測された文字入力間隔と前記記憶手段に登録された識別情報およびパスワードデータおよび文字入力間隔との間に所定の関係が成立するか否かにより、前記被認証者が本人であるか否かの認証を行なう認証手段とを具備している。

【００１６】さらに、本発明の個人認証装置は、登録時、被認証者を特定するための識別情報を入力する第１の識別情報入力手段と、登録用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力する第１のパスワード入力手段と、この第１のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第１の入力間隔計測手段と、文字入力間隔の許容誤差値を入力する許容誤差値入力手段と、前記第１の識別情報入力手段により入力された識別情報および前記第１のパスワード入力手段により入力されたパスワードデータおよび前記第１の入力間隔計測手段により計測された文字入力間隔および前記許容誤差値入力手段により入力された許容誤差値を登録データとして登録記憶する記憶手段と、照合時、被認証者を特定するための識別情報を入力する第２の識別情報入力手段と、照合用の被認証者の複数の文字からなるパスワードデータを１文字ずつ入力する第２のパスワード入力手段と、この第２のパスワード入力手段によるパスワードデータの入力時に各文字の入力間隔をそれぞれ計測する第２の入力間隔計測手段と、前記第２の識別情報入力手段により入力された照合用の識別情報および前記第２のパスワード入力手段により入力されたパスワードデータおよび前記第２の入力間隔計測手段により計測された文字入力間隔を前記記憶手段に登録された識別情報およびパスワードデータおよび文字入力間隔とそれぞれ照合する照合手段と、この照合手段の照合において、前記第２の識別情報入力手段により入力された照合用の識別情報および前記第２のパスワード入力手段により入力されたパスワードデータおよび前記第２の入力間隔計測手段により計測された文字入力間隔と前記記憶手段に登録された識別情報およびパスワードデータおよび文字入力間隔との間に所定の関係が成立し、かつ、前記第２の入力間隔計測手段により計測された文字入力間隔と前記記憶手段に登録された文字入力間隔とが前記記憶手段に登録された許容誤差値の範囲内で一致した場合に前記被認

証者が本人であると認証する認証手段とを具備している。

【００１７】本発明によれば、被認証者のパスワードデータ入力時における文字入力間隔をあらかじめ登録しておき、被認証者が行なうパスワードデータ入力の際にその文字入力間隔をそれぞれ計測して、あらかじめ登録された文字入力間隔と照合することにより、入力されたパスワードデータおよび計測された文字入力間隔と登録されたパスワードデータおよび文字入力間隔との間に所定の関係が成立するか否かによって、被認証者が本人であるか否かの認証を行なうことにより、本人へのなりすましによる不正使用を防止でき、個人認証の精度が著しく向上する。

【００１８】一般に、パスワードデータが盗み見などにより比較的容易に盗用され易いのに対して、この文字入力間隔は盗み見による盗用がほぼ不可能である。加えて、文字入力間隔の照合を行なっていること自体が極めて発見され難い。この２点から、本発明は極めて破られ難い個人認証方法であると言える。したがって、たとえば、利用許可者以外の操作による端末装置の不正使用を見抜き、かつ、不正使用を防止することができる。

【００１９】

【発明の実施の形態】まず、本発明の実施の形態を説明する前に、本発明の概要について簡単に説明しておく。前述したように、たとえば、現金の出入りを管理する現金処理機やキャッシュレジスタ、あるいは、機密情報を保管・表示・操作するパーソナルコンピュータなどの端末装置は、あらかじめ使用を許可された特定のオペレータ以外が不正に使用することを防止するため、使用に先立ちパスワードデータのチェックを行なうことが多い。このパスワードデータは、オペレータごとに定められていて、通常は数字や文字もしくはその両者の組合わせからなる。

【００２０】このような複数の文字から構成されるパスワードデータは、通常、キーボードなどの入力装置から１文字ずつ入力されるが、各文字間の入力間隔時間は、同一のオペレータが同一の文字列を入力する場合には、何度入力を行なってもほぼ同一であるという性質を持つ。言い換えれば、文字入力間隔にはオペレータの癖が出るということで、この性質は特に、同一の文字列入力を行なう回数が増えれば増えるほど強まり、文字入力間隔（時間）の入力ごとのばらつきは少なくなる傾向にある。

【００２１】本発明は、このような性質を利用して、パスワードデータの照合に加えて、パスワードデータの文字入力間隔を照合することにより、個人認証の精度を著しく向上するものである。

【００２２】以下、本発明の実施の形態について図面を参照して説明する。図１は、本実施の形態に係る個人認証方法および個人認証装置が適用される現金処理機の構成を概略的に示すものである。本実施の形態に係る現金処理機は、制御手段としてのＣＰＵ（セントラル・プロセッシング・ユニット）１、記憶手段としての不揮発性メモリ（たとえば、ＮＶＲＡＭ）２、入力手段としてのキーボード３、計時手段としてのタイマ４、および、表示手段としての表示部５、入出金部６、および、通信制御部７から構成されている。

【００２３】ＣＰＵ１は、前記各部をそれぞれ制御したり、データの入出力および演算や比較処理などを行なう。不揮発性メモリ２は、利用者（オペレータ）の従業員番号、パスワードデータ、パスワードデータの文字入力間隔、および、文字入力間隔の許容誤差値を保存（記憶）するパスワード管理エリアを有する。パスワード管理エリアは、たとえば、図２に示すように、従業員番号を記憶する従業員番号保存エリア１１、パスワードデータを記憶するパスワード保存エリア１２、文字入力間隔を記憶する入力間隔保存エリア１３、および、許容誤差値を記憶する許容誤差保存エリア１４から構成されている。

【００２４】キーボード３は、利用者の現金処理機への操作指示を行なうと共に、利用者を特定する識別情報としての従業員番号、個人認証を行なうためのパスワードデータ、および、パスワードデータの文字入力間隔の許容誤差値などを入力するもので、たとえば、図３に示すように、入金処理を選択する入金キー２１、出金処理を選択する出金キー２２、および、各種データの入力を行なうテンキー２３などが設けられている。

【００２５】タイマ４は、時刻情報を生成するもので、ＣＰＵ１からの指示を受けると、ミリ秒単位で現在の時刻をＣＰＵ１に出力する。表示部５は、利用者に対して現金処理機の操作に必要な情報などを表示出力する。

【００２６】入出金部６は、入金あるいは出金処理を選択的に行なう。通信制御部７は、図示しないホスト装置との間でオンライン交信を行なう。次に、上記のような構成において、図４および図５に示すフローチャートを参照して、パスワードデータおよびパスワードデータの文字入力間隔を登録する登録処理について説明する。なお、以下に説明する処理は、主にＣＰＵ１の制御によって実行される。

【００２７】まず、ステップＳ１にて、図６に示すようなパスワード入力督促画面を表示部５に表示し、たとえば、６桁の従業員番号および４桁のパスワードデータの入力を待機する。ここで、利用者が、まず自己の従業員番号をキーボード３から入力すると（Ｓ２）、この入力された従業員番号は、図２に示すように、不揮発性メモリ２のパスワード管理エリア内の従業員番号保存エリア１１に格納される（Ｓ３）。

【００２８】次に、利用者は、従業員番号に続いてパスワードデータの１文字目をキーボード３から入力すると（Ｓ４）、このときの時刻ｔ１がタイマ４から読取られ

るとともに（Ｓ５）、入力されたパスワードデータの１文字目が、図２に示すように、不揮発性メモリ２のパスワード管理エリア内のパスワード保存エリア１２に格納される（Ｓ６）。

【００２９】次に、利用者は、パスワードデータの２文字目をキーボード３から入力すると（Ｓ７）、このときの時刻ｔ2 をタイマ４から読取るとともに（Ｓ８）、入力されたパスワードデータの２文字目を、図２に示すように、不揮発性メモリ２のパスワード管理エリア内のパスワード保存エリア１２に格納する（Ｓ９）。

【００３０】次に、１文字目の入力時刻ｔ1 と２文字目の入力時刻ｔ2 との差分（ｔ2 －ｔ1 ）を取ることにより、第１入力間隔Δｔ1 を求め、この求めた第１入力間隔Δｔ1 を、図２に示すように、不揮発性メモリ２のパスワード管理エリア内の入力間隔保存エリア１３に格納する（Ｓ１０）。

【００３１】次に、利用者は、パスワードデータの３文字目をキーボード３から入力すると（Ｓ１１）、このときの時刻ｔ3 をタイマ４から読取るとともに（Ｓ１２）、入力されたパスワードデータの３文字目を、図２に示すように、不揮発性メモリ２のパスワード管理エリア内のパスワード保存エリア１２に格納する（Ｓ１３）。

【００３２】次に、２文字目の入力時刻ｔ2 と３文字目の入力時刻ｔ3 との差分（ｔ3 －ｔ2 ）を取ることにより、第２入力間隔Δｔ2 を求め、この求めた第２入力間隔Δｔ2 を、図２に示すように、不揮発性メモリ２のパスワード管理エリア内の入力間隔保存エリア１３に格納する（Ｓ１４）。

【００３３】次に、利用者は、パスワードデータの４文字目をキーボード３から入力すると（Ｓ１５）、このときの時刻ｔ4 をタイマ４から読取るとともに（Ｓ１６）、入力されたパスワードデータの４文字目を、図２に示すように、不揮発性メモリ２のパスワード管理エリア内のパスワード保存エリア１２に格納する（Ｓ１７）。

【００３４】次に、３文字目の入力時刻ｔ3 と４文字目の入力時刻ｔ4 との差分（ｔ4 －ｔ3 ）を取ることにより、第３入力間隔Δｔ3 を求め、この求めた第３入力間隔Δｔ3 を、図２に示すように、不揮発性メモリ２のパスワード管理エリア内の入力間隔保存エリア１３に格納する（Ｓ１８）。

【００３５】次に、図７に示すフローチャートを参照して、パスワードデータの文字入力間隔の許容誤差値を設定（登録）する第１の設定処理について説明する。なお、以下に説明する処理は、主にＣＰＵ１の制御によって実行される。

【００３６】まず、ステップＳ２１にて、図９に示すような許容誤差入力督促画面を表示部５に表示し、許容誤差値の入力を待機する。ここで、利用者が所定の許容誤差値（％）をキーボード３から入力すると（Ｓ２２）、この入力された許容誤差値は、図２に示すように、不揮発性メモリ２のパスワード管理エリア内の許容誤差値保存エリア１４に格納される（Ｓ２３）。

【００３７】次に、図８に示すフローチャートを参照して、パスワードデータの文字入力間隔の許容誤差値を設定（登録）する第２の設定処理について説明する。なお、以下に説明する処理は、主にＣＰＵ１の制御によって実行される。

【００３８】この第２の設定処理は、図７に示した基本的な設定処理（第１の設定処理）に対して、設定値の上限チェックおよび下限チェックを追加している。これは、許容誤差値の設定が大きすぎると、文字入力間隔の照合精度が緩みすぎ、本発明の効果が失なわれ、許容誤差値の設定が小さすぎると、文字入力間隔の照合精度が厳しくなり過ぎてばらつきを許容できず、不正使用でないのに不正使用と見なしてしまう、という考えに基づいている。

【００３９】まず、ステップＳ３１にて、図９に示すような許容誤差入力督促画面を表示部５に表示し、許容誤差値の入力を待機する。ここで、利用者が所定の許容誤差値（％）をキーボード３から入力すると（Ｓ３２）、この入力された許容誤差値があらかじめ設定される所定の上限値（たとえば、数値「５０」）よりも小さいか否かをチェックする（Ｓ３３）。

【００４０】このチェックの結果、数値「５０」よりも小さくなかった場合（Ｓ３４）、たとえば、数値「４９」を不揮発性メモリ２のパスワード管理エリア内の許容誤差値保存エリア１４に格納する（Ｓ３５）。

【００４１】ステップＳ３３のチェックの結果、数値「５０」よりも小さかった場合（Ｓ３４）、入力された許容誤差値があらかじめ設定される所定の下限値（たとえば、数値「１５」）よりも小さいか否かをチェックする（Ｓ３６）。

【００４２】このチェックの結果、数値「１５」よりも小さかった場合（Ｓ３７）、たとえば、数値「１５」を不揮発性メモリ２のパスワード管理エリア内の許容誤差値保存エリア１４に格納する（Ｓ３８）。

【００４３】ステップＳ３７のチェックの結果、数値「１５」よりも小さくなかった場合（Ｓ３７）、入力された許容誤差値を不揮発性メモリ２のパスワード管理エリア内の許容誤差値保存エリア１４に格納する（Ｓ３９）。

【００４４】次に、図１０ないし図１３に示すフローチャートを参照して、利用者が利用許可を受けた利用者か否かを調べるためのパスワードデータの照合を行なう照合処理について説明する。なお、以下に説明する処理は、主にＣＰＵ１の制御によって実行される。

【００４５】まず、ステップＳ４１にて、図６に示すようなパスワード入力督促画面を表示部５に表示し、たと

えば、６桁の従業員番号および４桁のパスワードデータの入力を待機する。ここで、利用者が、まず自己の従業員番号をキーボード３から入力すると（Ｓ４２）、この入力された従業員番号が不揮発性メモリ２のパスワード管理エリア内の従業員番号保存エリア１１に存在するか否かをチェックする（Ｓ４３）。

【００４６】このチェックの結果、入力された従業員番号と同一の従業員番号が従業員番号保存エリア１１に存在しなかった場合（Ｓ４４）、たとえば、図１４に示すような利用を拒否する旨の画面（利用拒否画面）を表示部５に表示する（Ｓ４５、図１３参照）。ここで、利用者がその表示を目視して、たとえば、キーボード３でいずれかのキーを押下することにより（Ｓ４６）、処理を終了する。

【００４７】ステップＳ４３のチェックの結果、入力された従業員番号と同一の従業員番号が従業員番号保存エリア１１に存在した場合（Ｓ４４）、入力された従業員番号が特定の番号（たとえば、「９９９９９９」）であるか否かをチェックする（Ｓ４７）。

【００４８】このチェックの結果、入力された従業員番号が特定の番号「９９９９９９」であった場合（Ｓ４８）、ステップＳ４９（図１３参照）に進む。次に、利用者は、従業員番号に続いてパスワードデータの４文字をキーボード３から入力すると（Ｓ４９）、この入力されたパスワードデータが不揮発性メモリ２のパスワード管理エリア内の先に入力された従業員番号に対応するパスワード保存エリア１２内のパスワードデータと一致するか否かをチェックする（Ｓ５０）。

【００４９】このチェックの結果、両パスワードデータが一致しなかった場合（Ｓ５１）、ステップＳ４５に進み、前述同様な動作を繰り返す。ステップＳ５０のチェックの結果、両パスワードデータが一致した場合（Ｓ５１）、周知の入金処理あるいは出金処理に進む（Ｓ５２）。

【００５０】このように、特定の従業員番号「９９９９９９」に対してのみ、パスワードデータの文字入力間隔の照合処理は行なわず、従来と同様なパスワードデータの照合処理だけを行なうものである。

【００５１】図１０に戻って、ステップＳ４７のチェックの結果、入力された従業員番号が特定の番号「９９９９９９」でなかった場合（Ｓ４８）、ステップＳ５３に進む。次に、利用者は、従業員番号に続いてパスワードデータの１文字目をキーボード３から入力すると（Ｓ５３）、このときの時刻ｔ１がタイマ４から読取られるとともに（Ｓ５４）、入力されたパスワードデータの１文字目が、不揮発性メモリ２のパスワード管理エリア内の先に入力された従業員番号に対応するパスワード保存エリア１２内のパスワードデータの１文字目と一致するか否かをチェックする（Ｓ５５）。

【００５２】このチェックの結果、両パスワードデータの１文字目が一致しなかった場合（Ｓ５６）、ステップＳ４５に進み、前述同様な動作を繰り返す。ステップＳ５５のチェックの結果、両パスワードデータの１文字目が一致した場合（Ｓ５６）、ステップＳ５７に進む。

【００５３】次に、利用者は、パスワードデータの２文字目をキーボード３から入力すると（Ｓ５７）、このときの時刻ｔ２をタイマ４から読取り（Ｓ５８）、１文字目の入力時刻ｔ１と２文字目の入力時刻ｔ２との差分（ｔ２－ｔ１）を取ることにより、第１入力間隔Δｔ１を求め、この求めた第１入力間隔Δｔ１を、不揮発性メモリ２のパスワード管理エリア内の先に入力された従業員番号に対応する入力間隔保存エリア１３内の第１入力間隔Δｔ１と比較（照合）を行ない、その両者間の誤差が許容誤差値保存エリア１３内の許容誤差値の範囲内に収まっているか否かをチェックする（Ｓ５９）。

【００５４】ここで、許容誤差値の範囲内に収まっているための条件式は、以下に示す通りである。

－（登録済み許容誤差値）≦｛ｔｎ+1－ｔｎ｝÷Δｔｎ－1｝×１００≧登録済み許容誤差値（ｎ＝１，２，３）

ステップＳ５９のチェックの結果、許容誤差値の範囲内に収まっていない場合（Ｓ６０）、ステップＳ４５に進み、前述同様な動作を繰り返す。ステップＳ５９のチェックの結果、許容誤差値の範囲内に収まっている場合（Ｓ６０）、入力されたパスワードデータの２文字目が、不揮発性メモリ２のパスワード管理エリア内の先に入力された従業員番号に対応するパスワード保存エリア１２内のパスワードデータの２文字目と一致するか否かをチェックする（Ｓ６１）。

【００５５】このチェックの結果、両パスワードデータの２文字目が一致しなかった場合（Ｓ６２）、ステップＳ４５に進み、前述同様な動作を繰り返す。ステップＳ６１のチェックの結果、両パスワードデータの２文字目が一致した場合（Ｓ６２）、ステップＳ６３に進む。

【００５６】次に、利用者は、パスワードデータの３文字目をキーボード３から入力すると（Ｓ６３）、このときの時刻ｔ３をタイマ４から読取り（Ｓ６４）、２文字目の入力時刻ｔ２と３文字目の入力時刻ｔ３との差分（ｔ３－ｔ２）を取ることにより、第２入力間隔Δｔ２を求め、この求めた第２入力間隔Δｔ２を、不揮発性メモリ２のパスワード管理エリア内の先に入力された従業員番号に対応する入力間隔保存エリア１３内の第２入力間隔Δｔ２と比較（照合）を行ない、その両者間の誤差が許容誤差値保存エリア１３内の許容誤差値の範囲内に収まっているか否かをチェックする（Ｓ６５）。

【００５７】このチェックの結果、許容誤差値の範囲内に収まっていない場合（Ｓ６６）、ステップＳ４５に進み、前述同様な動作を繰り返す。ステップＳ６５のチェックの結果、許容誤差値の範囲内に収まっている場合（Ｓ６６）、入力されたパスワードデータの３文字目

が、不揮発性メモリ２のパスワード管理エリア内の先に入力された従業員番号に対応するパスワード保存エリア１２内のパスワードデータの３文字目と一致するか否かをチェックする（Ｓ６７）。

【００５８】このチェックの結果、両パスワードデータの３文字目が一致しなかった場合（Ｓ６８）、ステップＳ４５に進み、前述同様な動作を繰り返す。ステップＳ６７のチェックの結果、両パスワードデータの３文字目が一致した場合（Ｓ６８）、ステップＳ６９に進む。

【００５９】次に、利用者は、パスワードデータの４文字目をキーボード３から入力すると（Ｓ６９）、このときの時刻ｔ４をタイマ４から読取り（Ｓ７０）、３文字目の入力時刻ｔ３と４文字目の入力時刻ｔ４との差分（ｔ４－ｔ３）を取ることにより、第３入力間隔Δｔ３を求め、この求めた第３入力間隔Δｔ３を、不揮発性メモリ２のパスワード管理エリア内の先に入力された従業員番号に対応する入力間隔保存エリア１３内の第３入力間隔Δｔ３と比較（照合）を行ない、その両者間の誤差が許容誤差値保存エリア１３内の許容誤差値の範囲内に収まっているか否かをチェックする（Ｓ７１）。

【００６０】このチェックの結果、許容誤差値の範囲内に収まっていない場合（Ｓ７２）、ステップＳ４５に進み、前述同様な動作を繰り返す。ステップＳ７１のチェックの結果、許容誤差値の範囲内に収まっている場合（Ｓ７２）、入力されたパスワードデータの４文字目が、不揮発性メモリ２のパスワード管理エリア内の先に入力された従業員番号に対応するパスワード保存エリア１２内のパスワードデータの４文字目と一致するか否かをチェックする（Ｓ７３）。

【００６１】このチェックの結果、両パスワードデータの４文字目が一致しなかった場合（Ｓ７４）、ステップＳ４５に進み、前述同様な動作を繰り返す。ステップＳ７３のチェックの結果、両パスワードデータの４文字目が一致した場合（Ｓ７４）、周知の入金処理あるいは出金処理に進む（Ｓ５２）。

【００６２】このように、まず、利用者を特定するために従業員番号の入力を利用者に求め、従業員番号が登録されたものであるか否かをチェックし、利用者を特定する。これ以降、パスワードデータの文字入力ごとにタイマ４から時刻を読出し、それぞれの差分をとることにより文字の入力間隔を求める。求めた文字入力間隔をあらかじめ登録済みの入力間隔とそれぞれ比較し、両者間の誤差があらかじめ登録済みの許容誤差値の範囲内に収まっているか否かをチェックする。これと同時に、入力されたパスワードデータが正しいものか否かのチェックを文字入力ごとに行なう。これらの各チェックを全てパスした場合にのみ、利用者（オペレータ）は本人であると認証して、入金処理あるいは出金処理を許可し、パスしなかった場合には、利用者は本人でないと認証して、利用を拒否する旨の画面を表示部５に表示し、入金処理あるいは出金処理は行なわない。

【００６３】以上説明したように、上記実施の形態によれば、利用者のパスワードデータの入力時における文字の入力間隔をあらかじめ登録しておき、利用者が現金処理機の利用に先立って行なうパスワードデータ入力の際に文字の入力間隔（時間）を計測して、両者を照合し、同一人物と認められた場合にのみ、現金処理機の利用を許可することにより、利用許可者以外の操作による現金処理機の不正使用を見抜ねき、かつ、不正使用を防止することができる。

【００６４】パスワードデータが盗み見などにより比較的容易に盗用され易いのに対して、この文字入力間隔は盗み見による盗用がほぼ不可能である。加えて、文字入力間隔の照合を行なっていること自体が極めて発見され難い。これらから、本発明は極めて破られ難い個人認証方法であると言える。

【００６５】利用者を特定するための識別情報（実施の形態では従業員番号だが、他に氏名なども考えられる）の入力に際しても、本発明の文字入力間隔照合を施すことにより、個人認証の精度がさらに向上する。

【００６６】特定の従業員番号（実施の形態では「９９９９９」）に対して、選択的に文字入力間隔の照合処理を施さない手段を設け、この従業員番号とパスワードデータを管理者用に割り当て、管理者のみに公開することにより、複数の管理者による機器の運用管理が可能になる。

【００６７】許容誤差値の入力において、許容誤差値の最大値（実施の形態では４９％）を設け、これを超える指定を禁止する手段を設けることにより、文字入力間隔の照合精度が落ち過ぎて本発明の効果が失われることを防止できる。

【００６８】許容誤差値の入力において、許容誤差値の最小値（実施の形態では１５％）を設け、これを下回る値の指定を禁止する手段を設けることにより、文字入力間隔の照合精度を上げ過ぎて不正使用でないにも拘らず、照合をパスできなくなることを防止できる。

【００６９】

【発明の効果】以上詳述したように本発明よれば、本人へのなりすましによる不正使用を防止でき、個人認証の精度が著しく向上する個人認証方法および個人認証装置を提供できる。

【図面の簡単な説明】

【図１】本発明の実施の形態に係る個人認証方法および個人認証装置が適用される現金処理機の構成を概略的に示すブロック図。

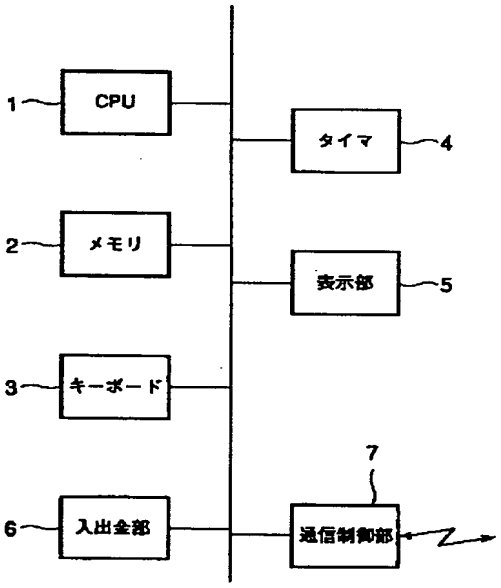
【図２】不揮発性メモリ内のパスワード管理エリアを説明する構成図。

【図３】キーボードの構成を示す平面図。

【図４】パスワードデータおよびパスワードデータの文字入力間隔を登録する登録処理を説明するフローチャー

ト。
【図５】パスワードデータおよびパスワードデータの文字入力間隔を登録する登録処理を説明するフローチャート。
【図６】パスワード入力督促画面の一例を示す平面図。
【図７】パスワードデータの文字入力間隔の許容誤差値を設定する第１の設定処理を説明するフローチャート。
【図８】パスワードデータの文字入力間隔の許容誤差値を設定する第２の設定処理を説明するフローチャート。
【図９】許容誤差入力督促画面の一例を示す平面図。
【図１０】パスワードデータの照合を行なう照合処理を説明するフローチャート。
【図１１】パスワードデータの照合を行なう照合処理を説明するフローチャート。
【図１２】パスワードデータの照合を行なう照合処理を説明するフローチャート。
【図１３】パスワードデータの照合を行なう照合処理を説明するフローチャート。
【図１４】利用拒否画面の一例を示す平面図。
【符号の説明】
１……ＣＰＵ、２……不揮発性メモリ、３……キーボード、４……タイマ、５……表示部、６……入出金部、７……通信制御部、１１……従業員番号保存エリア、１２……パスワード保存エリア、１３……入力間隔保存エリア、１４……許容誤差保存エリア。

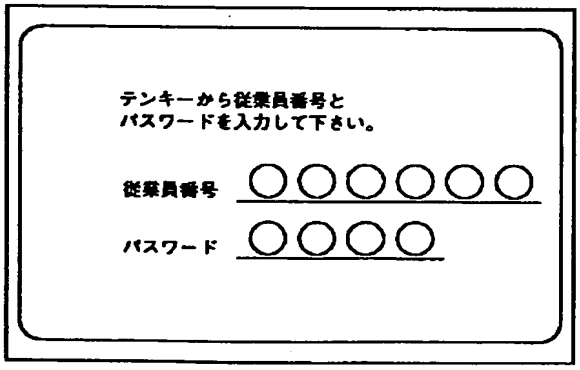
【図１】



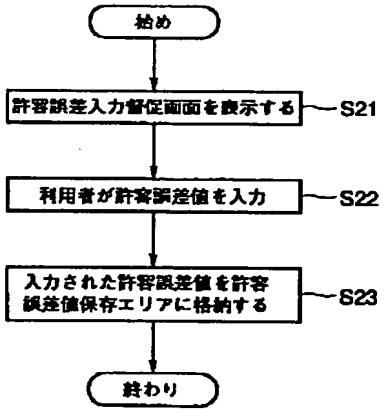
【図２】

従業員番号	パスワードデータ	文字入力間隔 (m sec)			許容誤差 (%)
		Δt1	Δt2	Δt3	
820458	5128	1383	1046	521	49
751099	0812	358	312	407	40
711415	0465	267	325	929	35
870278	1381	443	982	287	30
880848	1959	1172	473	821	15
999999	1129	0	0	0	0
		13			14
11	12				

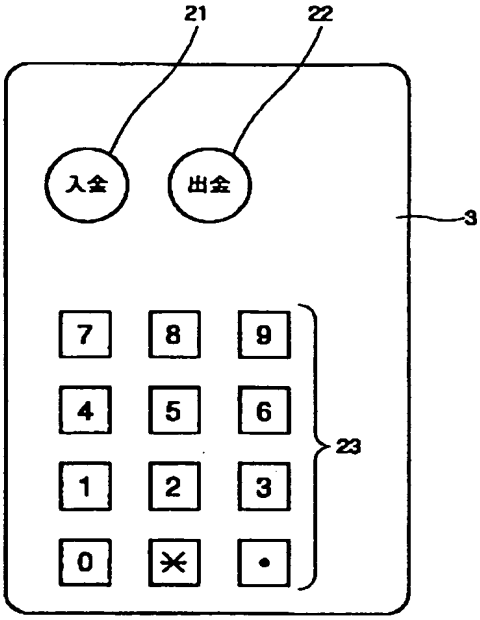
【図６】



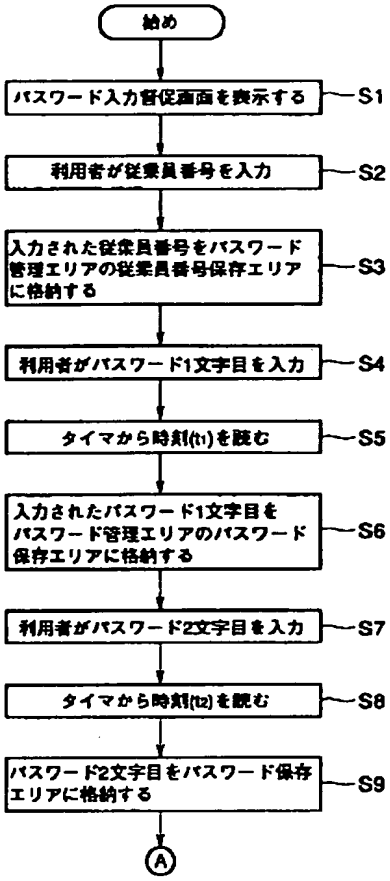
【図７】



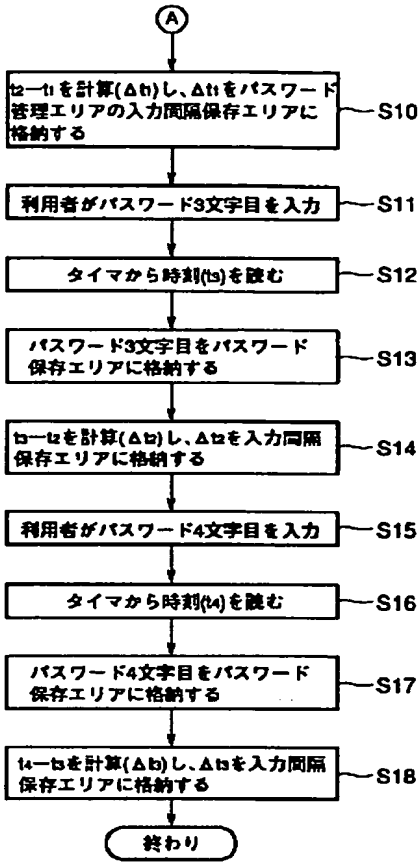
【図３】



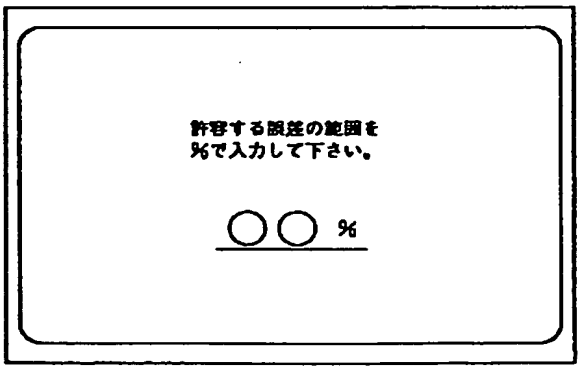
【図４】



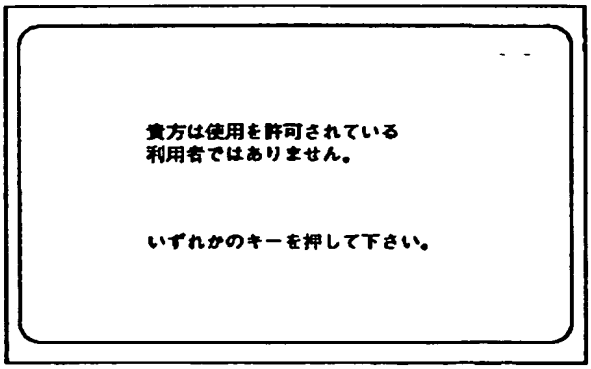
【図５】



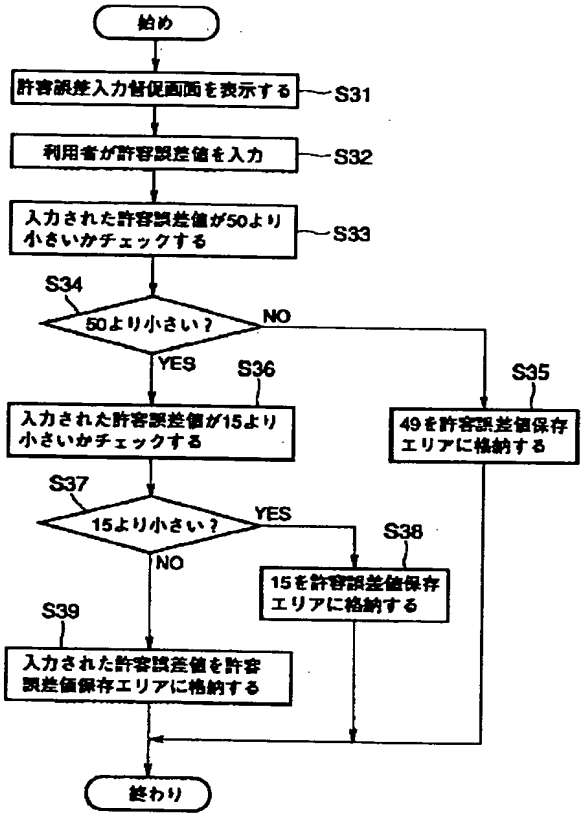
【図９】



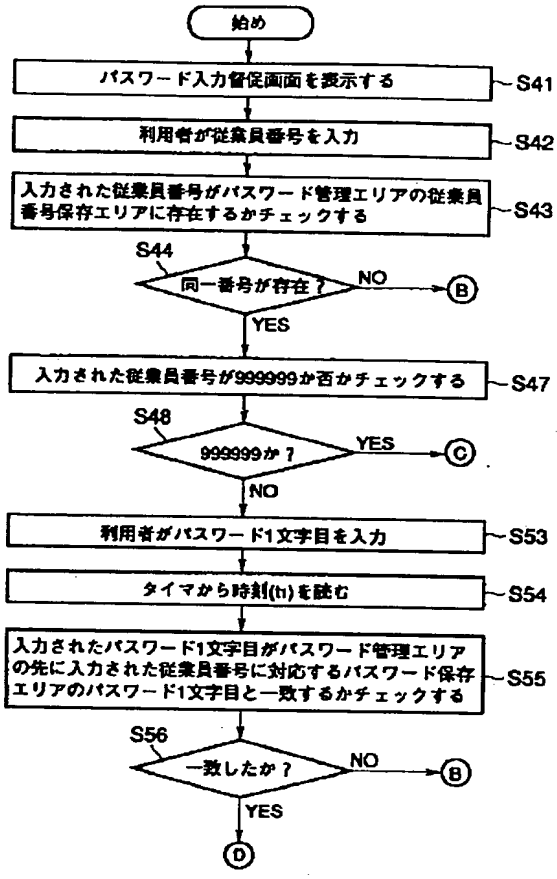
【図１４】



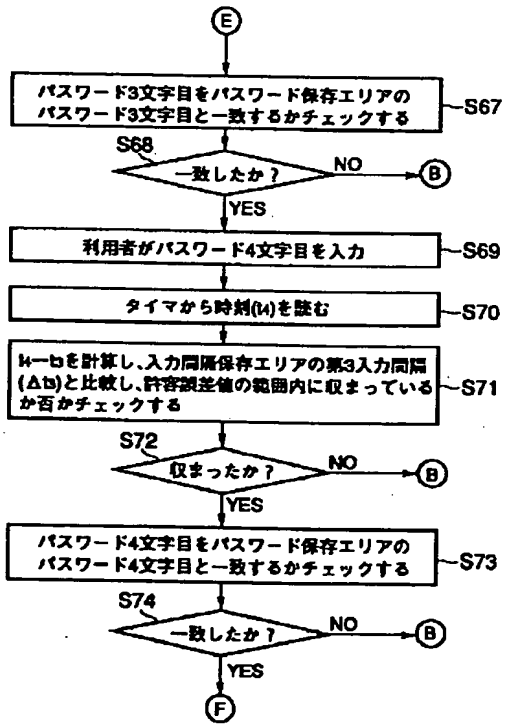
【図８】


始め
許容誤差入力督促画面を表示する
S31
利用者が許容誤差値を入力
S32
入力された許容誤差値が50より小さいかチェックする
S33
S34
50より小さい？
NO
YES
S36
入力された許容誤差値が15より小さいかチェックする
S35
49を許容誤差値保存エリアに格納する
S37
15より小さい？
YES
NO
S38
15を許容誤差値保存エリアに格納する
S39
入力された許容誤差値を許容誤差値保存エリアに格納する
終わり

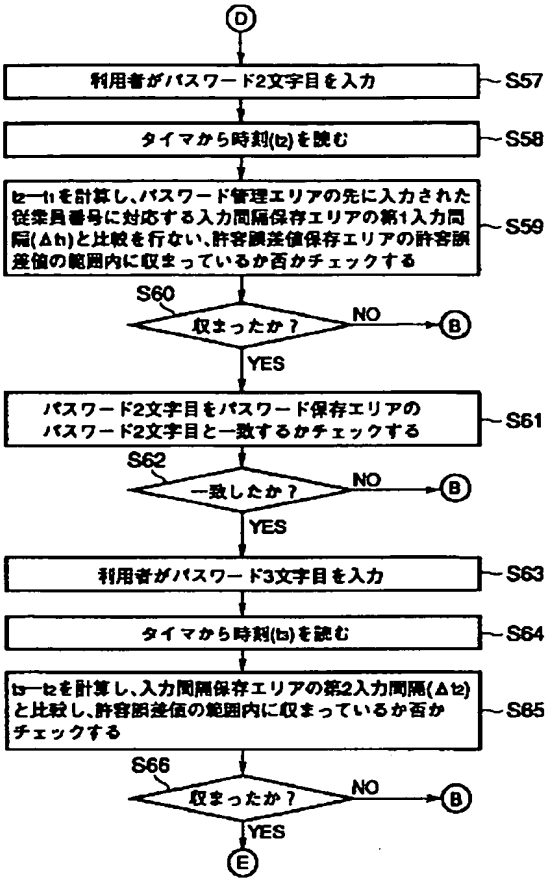
【図１０】


始め
パスワード入力督促画面を表示する
S41
利用者が従業員番号を入力
S42
入力された従業員番号がパスワード管理エリアの従業員番号保存エリアに存在するかチェックする
S43
S44
同一番号が存在？
NO
B
YES
入力された従業員番号が999999か否かチェックする
S47
S48
999999か？
YES
C
NO
利用者がパスワード1文字目を入力
S53
タイマから時刻(ti)を読む
S54
入力されたパスワード1文字目がパスワード管理エリアの先に入力された従業員番号に対応するパスワード保存エリアのパスワード1文字目と一致するかチェックする
S55
S56
一致したか？
NO
B
YES
D

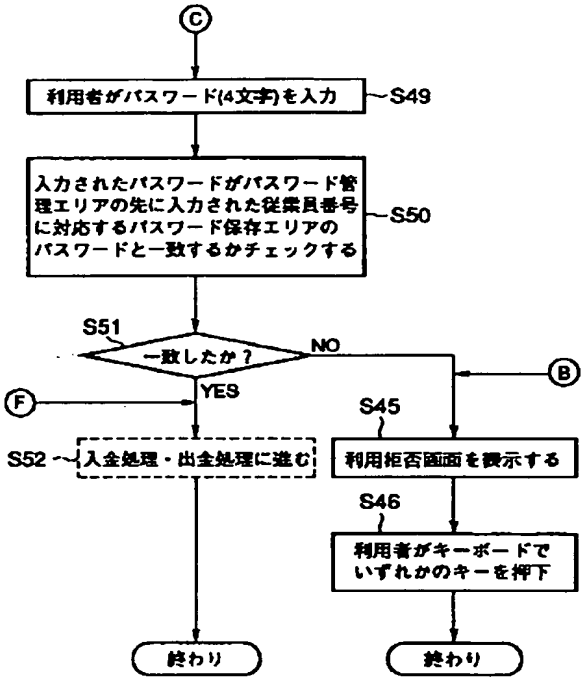
【図１２】


E
パスワード3文字目をパスワード保存エリアのパスワード3文字目と一致するかチェックする
S67
S68
一致したか？
NO
B
YES
利用者がパスワード4文字目を入力
S69
タイマから時刻(ti)を読む
S70
ti−tbを計算し、入力間隔保存エリアの第3入力間隔(Δtb)と比較し、許容誤差値の範囲内に収まっているか否かチェックする
S71
S72
収まったか？
NO
B
YES
パスワード4文字目をパスワード保存エリアのパスワード4文字目と一致するかチェックする
S73
S74
一致したか？
NO
B
YES
F

【図１１】


D
利用者がパスワード2文字目を入力
S57
タイマから時刻(t2)を読む
S58
t2−t1を計算し、パスワード管理エリアの先に入力された従業員番号に対応する入力間隔保存エリアの第1入力間隔(Δt1)と比較を行ない、許容誤差値保存エリアの許容誤差値の範囲内に収まっているか否かチェックする
S59
S60
収まったか？
NO
B
YES
パスワード2文字目をパスワード保存エリアのパスワード2文字目と一致するかチェックする
S61
S62
一致したか？
NO
B
YES
利用者がパスワード3文字目を入力
S63
タイマから時刻(t3)を読む
S64
t3−t2を計算し、入力間隔保存エリアの第2入力間隔(Δt2)と比較し、許容誤差値の範囲内に収まっているか否かチェックする
S65
S66
収まったか？
NO
B
YES
E

【図１３】


C
利用者がパスワード(4文字)を入力
S49
入力されたパスワードがパスワード管理エリアの先に入力された従業員番号に対応するパスワード保存エリアのパスワードと一致するかチェックする
S50
S51
一致したか？
NO
B
YES
F
S45
S52
入金処理・出金処理に進む
利用拒否画面を表示する
S46
利用者がキーボードでいずれかのキーを押下
終わり
終わり